# UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/774,079 | 02/06/2004 | Shehzad T. Merchant | 02453.0019.NPUS00 | 7139 |

27194      7590      02/02/2009
HOWREY LLP-CA
C/O IP DOCKETING DEPARTMENT
2941 FAIRVIEW PARK DRIVE, SUITE 200
FALLS CHURCH, VA 22042-2924

| EXAMINER |
|---|
| POPHAM, JEFFREY D |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2437 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 02/02/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

*Office Action Summary*

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

1)☒ Responsive to communication(s) filed on *30 October 2008*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

## Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## Remarks

Claims 1-45 are pending.

## Response to Arguments

1.     Applicant's arguments with respect to claims 1-45 have been considered but are moot in view of the new ground(s) of rejection.

## Claim Objections

2.     Claims 15, 23, 29, and 36 are objected to because of the following informalities:

- Claim 15 claims dependence on claim 4, however, claim 15 should apparently depend from claim 14.

- Claims 23 and 36 end after "a sequence of one or more vendor", but have been construed as continuing with "TLVs" as in claim 3.

- Claim 29 states that it is original, but has been changed to be a duplicate of claim 28.  For purposes of prior art rejection, claim 29 has been construed in its original form, as current claim 29 has already been rejected with respect to claim 28.

Appropriate correction is required.

## Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described
as set forth in section 102 of this title, if the differences between the subject matter sought to
be patented and the prior art are such that the subject matter as a whole would have been
obvious at the time the invention was made to a person having ordinary skill in the art to which
said subject matter pertains. Patentability shall not be negatived by the manner in which the
invention was made.

3.      Claims 1, 2, 4-6, 9, 10, 12-16, 18, 19, 21, 22, 24, 26, 39-42, and 45 are

rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart (U.S. Patent

6,732,176) in view of Lor (U.S. Patent Application Publication 2004/0068668).

Regarding Claim 1,

Stewart discloses a method of controlling access to a

network, comprising:

Requesting an identity from a client attempting to connect to

the network (Column 10, line 64 to Column 11, line 16);

Receiving the identity (Column 10, line 64 to Column 11, line

16);

Associating location information with the identity (Column 11,

lines 17-53);

Authenticating the identity (Column 9, lines 28-47; Column

12, line 30 to Column 13, line 10; and Column 18, lines 1-25);

Comparing the location information against a policy

designating locations, if any, at which the client is permitted to

connect to the network (Column 11, lines 28-53; and Column 16,

lines 38-64);

Deciding whether to grant or deny the client access to the

network based on the authenticity of the identity and the

comparison of the location information (Column 11, lines 28-53;

and Column 15, line 16 to Column 16, line 64);

Wherein if the client is granted access to the network, and

subsequently moves to a new location, the client continues to have

access to the network after moving to the new location, the client's

access at the new location will be based on policies of the new

location (Column 11, lines 28-53; and Column 15, line 16 to

Column 16, line 64);

But may not explicitly disclose that the network follows a

procedure to either re-authenticate or not re-authenticate the client

if the client subsequently moves to a new location.

Lor, however, discloses that the network follows a procedure

to either re-authenticate or not re-authenticate the client if the client

subsequently moves to a new location, and providing location-

based access control policies (Paragraphs 49, 54, and 63-72). It

would have been obvious to one of ordinary skill in the art at the

time of applicant's invention to incorporate the wireless LAN

switching system of Lor into the distributed network access system

of Stewart in order to provide additional levels of access control,

authentication, and authorization, such that access may be

controlled by client identity, time, location, and application and/or to

provide ease in re-association when a client moves from one

location to another.

Regarding Claim 39,

Claim 39 is a system claim that corresponds to method claim

1 and is rejected for the same reasons.

Regarding Claim 2,

Stewart as modified by Lor discloses the method of claim 1,

in addition, Stewart discloses passing the identity and the location

information to an authentication server, wherein the authentication

server performs the steps of authenticating, comparing and

deciding (Column 10, line 64 to Column 11, line 16; and Column

14, lines 40-56; authentication server being MIB or other device);

and Lor discloses passing the identity and the location information

to an authentication server, wherein the authentication server

performs the steps of authenticating, comparing and deciding

(Paragraphs 63-72).

Regarding Claim 4,

Stewart as modified by Lor discloses the method of claim 1,

in addition, Stewart discloses that the identity includes information

selected from the group consisting of a user name, a user

password, a certificate, a MAC address, a shared encryption key, a

smart card identifier, and any combination of the foregoing

information (Column 10, lines 53-63).

Regarding Claim 40,

Claim 40 is a system claim that corresponds to method claim

4 and is rejected for the same reasons.

Regarding Claim 5,

Stewart as modified by Lor discloses the method of claim 1,

in addition, Stewart discloses that the client station is a user station

capable of connecting to the network through an access point

(Column 10, line 64 to Column 11, line 16).

Regarding Claim 41,

Claim 41 is a system claim that corresponds to method claim

5 and is rejected for the same reasons.

Regarding Claim 6,

Stewart as modified by Lor discloses the method of claim 1,

in addition, Stewart discloses that the client is a wired device

capable of connecting to the network through an Ethernet switch

port (Column 5, lines 2-24; Column 6, lines 40-59; and Column 9,

lines 48-64).

Regarding Claim 42,

Claim 42 is a system claim that corresponds to method claim

6 and is rejected for the same reasons.

Regarding Claim 9,

Stewart as modified by Lor discloses the method of claim 1,

in addition, Stewart discloses that the location information indicates

the location of an edge device for connecting the client to the

network (Column 10, line 64 to Column 11, line 16).

Regarding Claim 45,

Claim 45 is a system claim that corresponds to method claim

9 and is rejected for the same reasons.

Regarding Claim 10,

Stewart discloses a network system, comprising:

An authenticator for requesting an identity from a client and

for associating location information with the identity (Column 10,

line 64 to Column 11, line 16);

An authentication server, receiving the identity and

associated location information from the authenticator, for deciding

whether to grant or deny the client access to the network based on

the identity and the location information (Column 9, lines 28-47;

Column 12, line 30 to Column 13, line 10; Column 14, lines 40-56;

Column 16, lines 38-55; and Column 18, lines 1-25);

Wherein if the client is granted access to the network, and

subsequently moves to a new location, the client continues to have

access to the network after moving to the new location, the client's

access at the new location will be based on policies of the new

location (Column 11, lines 28-53; and Column 15, line 16 to

Column 16, line 64);

But may not explicitly disclose that the network follows a

procedure to either re-authenticate or not re-authenticate the client

if the client subsequently moves to a new location.

Lor, however, discloses that the network system follows a

procedure to either re-authenticate or not re-authenticate the client

if the client subsequently moves to a new location, and providing

location-based access control policies (Paragraphs 49, 54, and 63-

72). It would have been obvious to one of ordinary skill in the art at

the time of applicant's invention to incorporate the wireless LAN

switching system of Lor into the distributed network access system

of Stewart in order to provide additional levels of access control,

authentication, and authorization, such that access may be

controlled by client identity, time, location, and application and/or to

provide ease in re-association when a client moves from one

location to another.

Regarding Claim 12,

Stewart as modified by Lor discloses the system of claim 10,

in addition, Stewart discloses that the authenticator resides in an

edge device (Column 10, line 64 to Column 11, line 16).

Regarding Claim 13,

Stewart as modified by Lor discloses the system of claim 10,

in addition, Stewart discloses an edge device for connecting a user

station to a network switch (Figures 2-3).

Regarding Claim 14,

Stewart as modified by Lor discloses the system of claim 13,

in addition, Stewart discloses that the edge device is a wireless

access point (Column 10, line 64 to Column 11, line 16).

Regarding Claim 15,

Stewart as modified by Lor discloses the system of claim 14,

in addition, Stewart discloses that the user is capable of connecting

to the network through the access point (Column 5, lines 1-14; and

Column 10, line 64 to Column 11, line 16).

Regarding Claim 16,

Stewart as modified by Lor discloses the system of claim 10,

in addition, Stewart discloses that the client is a wired device

capable of connecting to a network switch through an Ethernet port

(Column 5, lines 2-24; Column 6, lines 40-59; and Column 9, lines

48-64).

Regarding Claim 18,

Stewart as modified by Lor discloses the system of claim 10,

in addition, Stewart discloses that the location information indicates

the location of an edge device for connecting the client to the

network (Column 10, line 64 to Column 11, line 16).

Regarding Claim 19,

Stewart as modified by Lor discloses the system of claim 18,

in addition, Lor discloses an interface for permitting an

administrator to associate the location information to the edge

device (Paragraphs 54-55 and 99-104).

Regarding Claim 21,

Stewart as modified by Lor discloses the system of claim 10,

in addition, Stewart discloses that the authentication server

authenticates the identity (Column 9, lines 28-47; Column 12, line

30 to Column 13, line 10; Column 14, lines 40-56; Column 16, lines

38-55; and Column 18, lines 1-25); and Lor discloses that the

authentication server authenticates the identity (Paragraphs 63-72).

Regarding Claim 22,

Stewart as modified by Lor discloses the system of claim 10,

in addition, Stewart discloses that the authentication server

includes a policy designating locations, if any, at which the client is

permitted to connect to the network (Column 11, lines 28-53; and

Column 16, lines 38-64).

Regarding Claim 24,

Stewart as modified by Lor discloses the system of claim 10,

in addition, Stewart discloses that the identity information includes

information selected from the group consisting of a user name, a

user password, a certificate, a MAC address, a shared key, a smart

card identifier, and any combination of the foregoing information

(Column 10, lines 53-63).

Regarding Claim 26,

Stewart as modified by Lor discloses the system of claim 10,

in addition, Lor discloses that the authentication server comprises

an authentication mechanism selected from the group consisting of

TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of

the foregoing (Paragraphs 42-44).

4.      Claims 3, 7, 23, 25, and 43 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Stewart in view of Lor, further in view of Funk (Funk Software,

"Comprehensive RADIUS/AAA Solution for the Global Enterprise", 2/22/2003,

pp. 1-6).

Regarding Claim 3,

Stewart as modified by Lor does not explicitly disclose

operating the authentication server which is a RADIUS server that

operates with Steel-Belted Radius, Enterprise Edition; wherein

RADIUS attributes of an access request packet are defined as type

length values that contain additional information; and wherein

vendor specific attributes indicate a vendor ID and a sting field

encoding a sequence of one or more vendor type length values.

Funk, however, discloses operating the authentication server

which is a RADIUS server that operates with Steel-Belted Radius,

Enterprise Edition; wherein RADIUS attributes of an access request

packet are defined as type length values that contain additional

information; and wherein vendor specific attributes indicate a

vendor ID and a sting field encoding a sequence of one or more

vendor type length values (Pages 1-6; seen both in the text of the

document and the RFC compliance portion, for example, referring

to providing compliance with RFC2548, cited by applicant and titled

"Microsoft Vendor-specific RADIUS Attributes"). It would have

been obvious to one of ordinary skill in the art at the time of

applicant's invention to incorporate the AAA system of Funk into the

distributed network access system of Stewart as modified by Lor in

order to allow the system to centralize security and access controls,

such as authentication, authorization, and accounting, manage the

busiest of networks, scale to accommodate growing networks,

and/or to provide high reliability and uptime.

Regarding Claim 7,

Stewart as modified by Lor does not explicitly disclose using

as an authentication mechanism an MD5 protocol to authenticate

the identity.

Funk, however, discloses using as an authentication

mechanism an MD5 protocol to authenticate the identity (Page 3).

It would have been obvious to one of ordinary skill in the art at the

time of applicant's invention to incorporate the AAA system of Funk

into the distributed network access system of Stewart as modified

by Lor in order to allow the system to centralize security and access

controls, such as authentication, authorization, and accounting,

manage the busiest of networks, scale to accommodate growing

networks, and/or to provide high reliability and uptime.

Regarding Claim 43,

Claim 43 is a system claim that corresponds to method claim

7 and is rejected for the same reasons.

Regarding Claim 23,

Stewart as modified by Lor does not explicitly disclose the

authentication server is a RADIUS server that operates with Steel-

Belted Radius, Enterprise Edition; wherein RADIUS attributes of an

access request packet are defined as type length values that

contain additional information; and wherein vendor specific

attributes indicate a vendor ID and a sting field encoding a

sequence of one or more vendor type length values.

Funk, however, discloses the authentication server is a

RADIUS server that operates with Steel-Belted Radius, Enterprise

Edition; wherein RADIUS attributes of an access request packet

are defined as type length values that contain additional

information; and wherein vendor specific attributes indicate a

vendor ID and a sting field encoding a sequence of one or more

vendor type length values (Pages 1-6; seen both in the text of the

document and the RFC compliance portion, for example, referring

to providing compliance with RFC2548, cited by applicant and titled

"Microsoft Vendor-specific RADIUS Attributes"). It would have

been obvious to one of ordinary skill in the art at the time of

applicant's invention to incorporate the AAA system of Funk into the

distributed network access system of Stewart as modified by Lor in

order to allow the system to centralize security and access controls,

such as authentication, authorization, and accounting, manage the

busiest of networks, scale to accommodate growing networks,

and/or to provide high reliability and uptime.

Regarding Claim 25,

Stewart as modified by Lor does not explicitly disclose a

network switch that comprises an authentication mechanism

comprising an MD5 protocol for authenticating the identity.

Funk, however, discloses a network switch that comprises

an authentication mechanism comprising an MD5 protocol for

authenticating the identity (Page 3). It would have been obvious to

one of ordinary skill in the art at the time of applicant's invention to

incorporate the AAA system of Funk into the distributed network

access system of Stewart as modified by Lor in order to allow the

system to centralize security and access controls, such as

authentication, authorization, and accounting, manage the busiest

of networks, scale to accommodate growing networks, and/or to

provide high reliability and uptime.

5.      Claims 8, 17, and 44 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Stewart in view of Lor, further in view of Liming (U.S. Patent

Application Publication 2002/0055924).

Regarding Claim 8,

Stewart as modified by Lor does not explicitly disclose that

the location information indicates the location of a network switch to

which the client is attempting to connect.

Liming, however, discloses that the location information

indicates the location of a network switch to which the client is

attempting to connect (Paragraph 159).  It would have been

obvious to one of ordinary skill in the art at the time of applicant's

invention to incorporate the location context system of Liming into

the distributed network access system of Stewart as modified by

Lor in order to allow the system to associate location information

with the client even when the other devices cannot provide such

location information, thereby extending the system to be able to be

used when the client connects directly to a switch and/or when the

other devices between the client and switch do not have any means

to associate location information with the client.

Regarding Claim 44,

Claim 44 is a system claim that corresponds to method claim

8 and is rejected for the same reasons.

Regarding Claim 17,

Stewart as modified by Lor does not explicitly disclose that

the location information indicates the location of a network switch to

which the client is attempting to connect.

Liming, however, discloses that the location information

indicates the location of a network switch to which the client is

attempting to connect (Paragraph 159). It would have been

obvious to one of ordinary skill in the art at the time of applicant's

invention to incorporate the location context system of Liming into

the distributed network access system of Stewart as modified by

Lor in order to allow the system to associate location information

with the client even when the other devices cannot provide such

location information, thereby extending the system to be able to be

used when the client connects directly to a switch and/or when the

other devices between the client and switch do not have any means

to associate location information with the client.


6.      Claims 11, 20, 27-29, 31-35, and 37 are rejected under 35 U.S.C. 103(a)

as being unpatentable over Stewart in view of Lor, further in view of Kwan (U.S.

Patent Application Publication 2004/0255154).

Regarding Claim 11,

Stewart as modified by Lor does not explicitly disclose that

the authenticator resides in a network switch.

Kwan, however, discloses that the authenticator resides in a network switch (Paragraph 56). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the multi-tiered network security system of Kwan into the distributed network access system of Stewart as modified by Lor in order to ensure that a client and it's associated user are authentic and authorized to use the system by three levels of security checks, including physical address authentication of the device, user credential authentication, and VLAN group association checks, thereby increasing security of the system.

Regarding Claim 20,

Stewart as modified by Lor does not explicitly disclose that the authentication server is included in a network switch.

Kwan, however, discloses that the authentication server is included in a network switch (Paragraph 36). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the multi-tiered network security system of Kwan into the distributed network access system of Stewart as modified by Lor in order to ensure that a client and it's associated user are authentic and authorized to use the system by three levels of security checks, including physical address authentication of the device, user credential authentication, and VLAN group association checks, thereby increasing security of the system.

Regarding Claim 27,

Stewart discloses a network system, comprising:

A plurality of edge devices capable of communicating with a
plurality of user stations over one or more wireless channels
(Column 10, line 64 to Column 11, line 16 );

A network switch including a plurality of ports for connecting
the edge devices to a network (Figures 2-3; and Column 9, lines
52-64);

An application for requesting station identities from the user
stations and for associating location information with each of the
station identities (Column 10, line 64 to Column 11, line 53);

An authentication server for deciding whether to grant or
deny each of the user stations access to the network based on the
corresponding identity and location information (Column 9, lines 28-
47; Column 12, line 30 to Column 13, line 10; Column 14, lines 40-
56; Column 16, lines 38-55; and Column 18, lines 1-25);

Wherein if the client is granted access to the network, and
subsequently moves to a new location, the client continues to have
access to the network after moving to the new location, the client's
access at the new location will be based on policies of the new
location (Column 11, lines 28-53; and Column 15, line 16 to
Column 16, line 64);

But may not explicitly disclose that the application is run on the network switch or that the network follows a procedure to either re-authenticate or not re-authenticate the client if the client subsequently moves to a new location.

Lor, however, discloses that the network system follows a procedure to either re-authenticate or not re-authenticate the client if the client subsequently moves to a new location, and providing location-based access control policies (Paragraphs 49, 54, and 63-72). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the wireless LAN switching system of Lor into the distributed network access system of Stewart in order to provide additional levels of access control, authentication, and authorization, such that access may be controlled by client identity, time, location, and application and/or to provide ease in re-association when a client moves from one location to another.

Kwan, however, discloses an application running on a network switch, for requesting station identities from user stations (Paragraph 56). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the multi-tiered network security system of Kwan into the distributed network access system of Stewart as modified by Lor in order to ensure that a client and it's associated user are authentic and authorized to use

the system by three levels of security checks, including physical

address authentication of the device, user credential authentication,

and VLAN group association checks, thereby increasing security of

the system.

Regarding Claim 28,

Stewart as modified by Lor and Kwan discloses the system

of claim 27, in addition, Stewart discloses that at least one of the

edge devices is a wireless access point (Column 10, line 64 to

Column 11, line 16).

Regarding Claim 29,

Stewart as modified by Lor and Kwan discloses the system

of claim 27, in addition, Kwan discloses a user station that is a

wired device for directly connecting one of the ports of the network

switch (Figure 1; and Paragraph 35).

Regarding Claim 31,

Stewart as modified by Lor and Kwan discloses the system

of claim 27, in addition, Stewart discloses that the location

information indicates the location of one of the edge devices

(Column 10, line 64 to Column 11, line 16).

Regarding Claim 32,

Stewart as modified by Lor and Kwan discloses the system

of claim 27, in addition, Lor discloses that the network switch

includes an interface for permitting an administrator to associate

the location information to the edge devices (Paragraphs 54-55 and 99-104).

Regarding Claim 33,

Stewart as modified by Lor and Kwan discloses the system of claim 27, in addition, Kwan discloses that the network switch includes an authenticator for authenticating the station identities (Paragraph 56).

Regarding Claim 34,

Stewart as modified by Lor and Kwan discloses the system of claim 27, in addition, Stewart discloses that the authentication server authenticates the station identities (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; Column 14, lines 40-56; Column 16, lines 38-55; and Column 18, lines 1-25); and Lor discloses that the authentication server authenticates the identities (Paragraphs 63-72).

Regarding Claim 35,

Stewart as modified by Lor and Kwan discloses the system of claim 27, in addition, Stewart discloses that the authentication server includes a policy designating locations, if any, at which the user stations are permitted to connect to the network (Column 11, lines 28-53; and Column 16, lines 38-64).

Regarding Claim 37,

Stewart as modified by Lor and Kwan discloses the system

of claim 27, in addition, Stewart discloses that the station identities

includes information selected from the group consisting of a user

name, a user password, a certificate, a MAC address, a shared

key, a smart card identifier, and any combination of the foregoing

information (Column 10, lines 53-65).

7.      Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Stewart in view of Lor and Kwan, further in view of Liming.

Stewart as modified by Lor and Kwan does not explicitly disclose

that the location information indicates the location of the network switch.

Liming, however, discloses that the location information indicates

the location of the network switch (Paragraph 159).  It would have been

obvious to one of ordinary skill in the art at the time of applicant's invention

to incorporate the location context system of Liming into the distributed

network access system of Stewart as modified by Lor and Kwan in order

to allow the system to associate location information with the client even

when the other devices cannot provide such location information, thereby

extending the system to be able to be used when the client connects

directly to a switch and/or when the other devices between the client and

switch do not have any means to associate location information with the

client.

8.      Claims 36 and 38 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Stewart in view of Lor and Kwan, further in view of Funk.

        Regarding Claim 36,

                Stewart as modified by Lor and Kwan does not explicitly

        disclose the authentication server is a RADIUS server that operates

        with Steel-Belted Radius, Enterprise Edition; wherein RADIUS

        attributes of an access request packet are defined as type length

        values that contain additional information; and wherein vendor

        specific attributes indicate a vendor ID and a sting field encoding a

        sequence of one or more vendor type length values.

                Funk, however, discloses the authentication server is a

        RADIUS server that operates with Steel-Belted Radius, Enterprise

        Edition; wherein RADIUS attributes of an access request packet

        are defined as type length values that contain additional

        information; and wherein vendor specific attributes indicate a

        vendor ID and a sting field encoding a sequence of one or more

        vendor type length values (Pages 1-6; seen both in the text of the

        document and the RFC compliance portion, for example, referring

        to providing compliance with RFC2548, cited by applicant and titled

        "Microsoft Vendor-specific RADIUS Attributes"). It would have

        been obvious to one of ordinary skill in the art at the time of

        applicant's invention to incorporate the AAA system of Funk into the

        distributed network access system of Stewart as modified by Lor

and Kwan in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

Regarding Claim 38,

Stewart as modified by Lor and Kwan does not explicitly disclose an authentication mechanism comprising an MD5 protocol for authenticating the identity.

Funk, however, discloses an authentication mechanism comprising an MD5 protocol for authenticating the identity (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Lor and Kwan in order to allow the system to centralize security and access controls, such as authentication, authorization, and accounting, manage the busiest of networks, scale to accommodate growing networks, and/or to provide high reliability and uptime.

## *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**.

See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from

the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public

PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-

9199 (IN USA OR CANADA) or 571-272-1000.


                                        Jeffrey D Popham
                                        Examiner
                                        Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437